Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 24 April 2023 – Monday 15 May 2023

Supervised hours 5 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part A

You must have:
Risk_Assessment.rtf
Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- Learners must only have access to **Part A** during this supervised assessment period.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- **Part B** materials must not be accessed during completion of **Part A**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 43.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete **Part A** on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in **Part A** but cannot provide any guidance in completion of the activities.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learners' work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely, and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A**, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 15 May 2023.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is **not** allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in **Part A** but cannot provide any guidance in completion of the activities.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within this folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

The Eighties Hotel

Peter Okdekaj is the owner of a hotel chain, Okdekaj Hotels Group (OHG). Each hotel is themed on different historical periods, e.g. Edwardian or Victorian.

Peter has recently purchased another building that he is going to develop into a hotel themed on the 1980s.

The building was constructed in 1985. It is a six-floor apartment block. There is a shopping arcade on the ground floor, an underground car park and five accommodation floors. The ground floor shopping arcade will be made into offices, a reception area, a restaurant, and other public amenities.

Figure 1 shows a map of the area. There are public roads on all four sides. The building is in a large town and is surrounded by shops and offices on three sides. There is a public park at the back of the building.

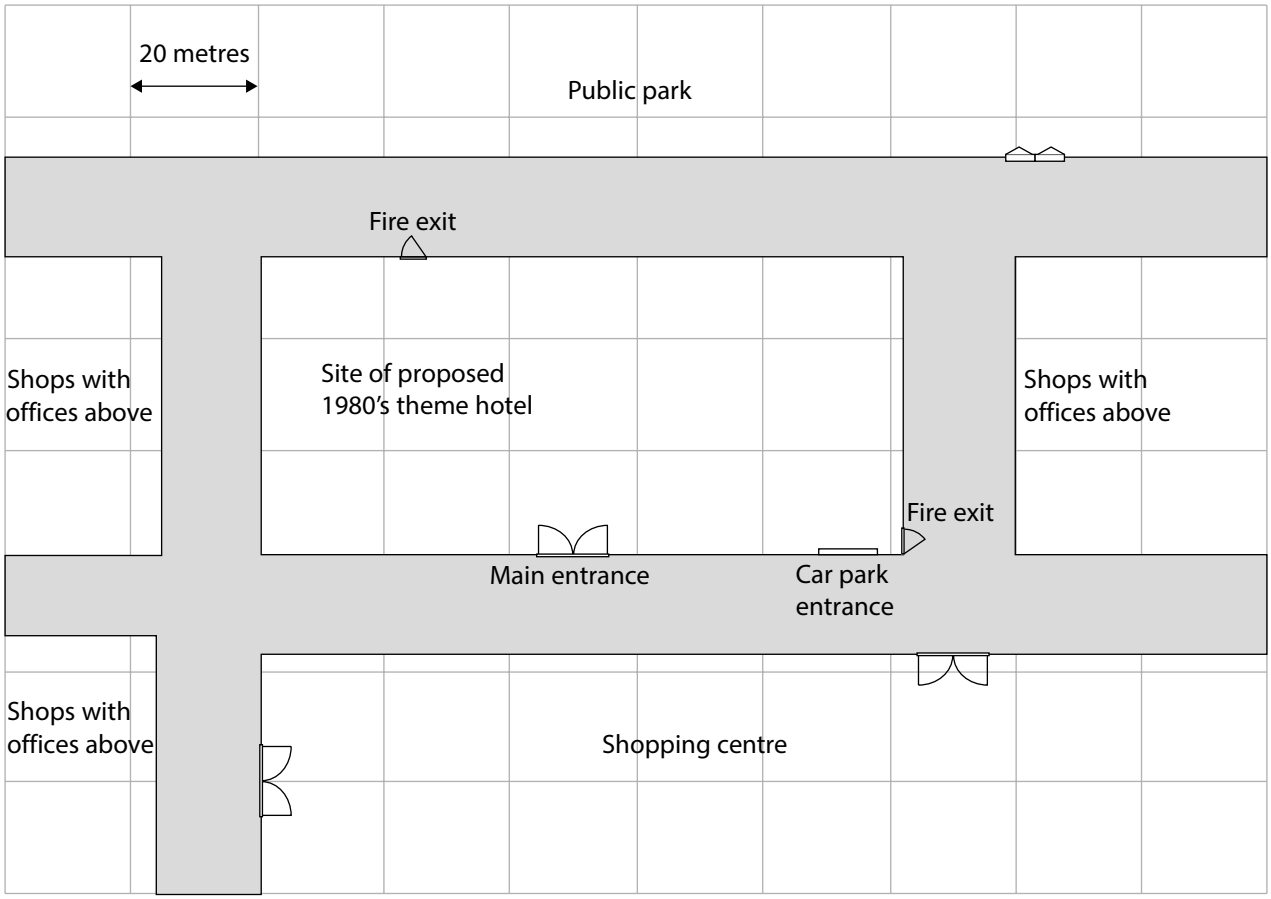

Figure 1

The five accommodation floors will all have the same layout. **Figure 2** shows the floor plan of one accommodation floor and the ground floor. There will be 12 guest rooms on each floor. The centre of the hotel is a light well, an open space with balconies on each floor and a glass roof.

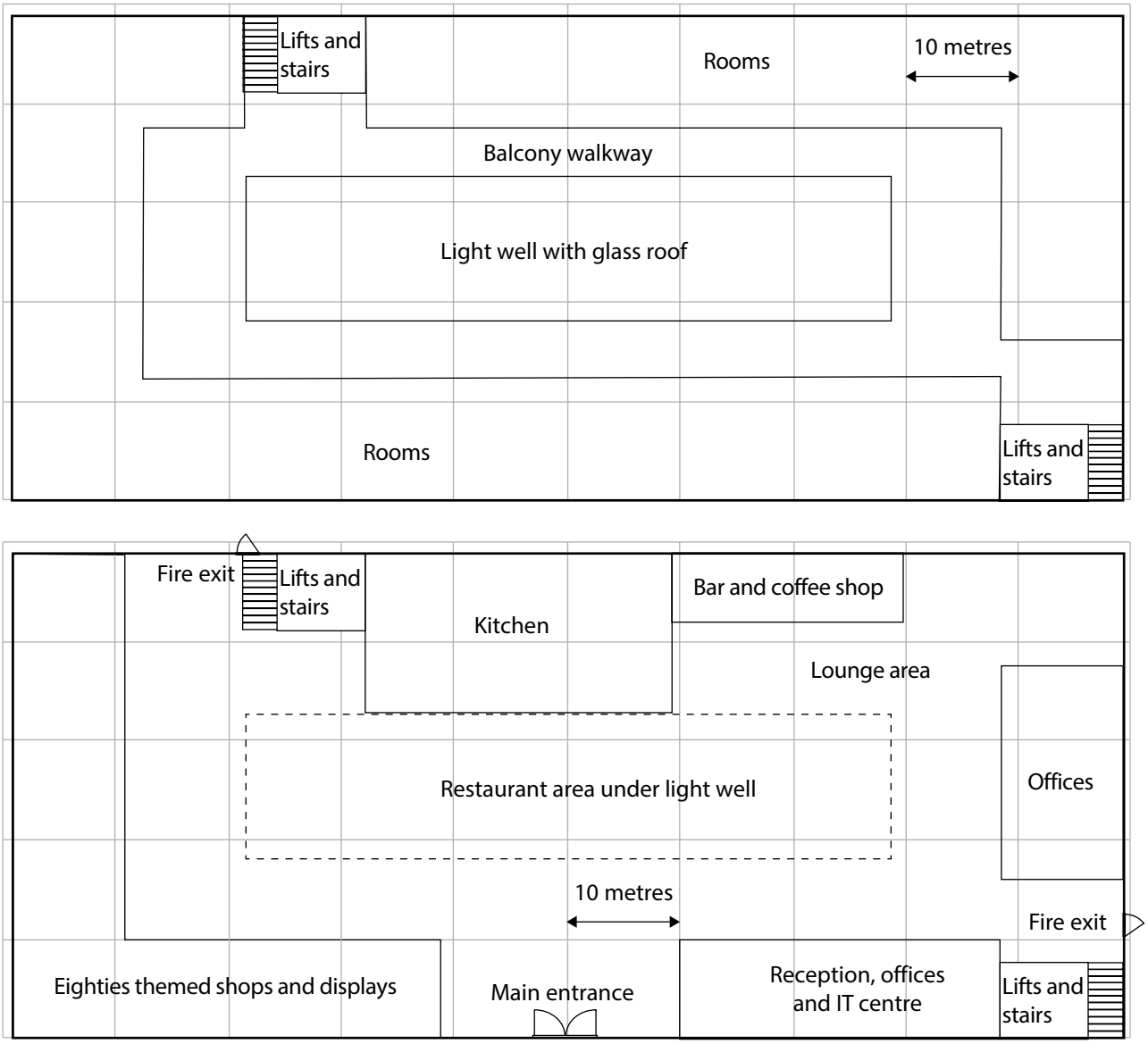

Figure 2

In keeping with the Eighties theme, each guest room will have an entertainment centre that will provide 1980s films, music, TV programmes and computer facilities.

The films, music and TV will be streamed from a media server.

As WiFi and the internet were not available before the 1990s, there will not be any guest WiFi in the hotel and the internet will only be available through guests' own devices.

The 1980s' computer facilities will be supplied by virtual machines running on a dedicated server. These virtual machines will emulate IBM compatible 386 machines from 1986. They would have been high end, home PCs in the 1980s.

The operating system will be the Microsoft Disk Operating System (MS-DOS) version 3.2

MS-DOS 3.2 uses a command line interface and was introduced in 1986. It allows networking and supports 3.5-inch, 720 KB floppy drives.

Figure 3 shows Peter's outline plan for the IT system in the hotel.

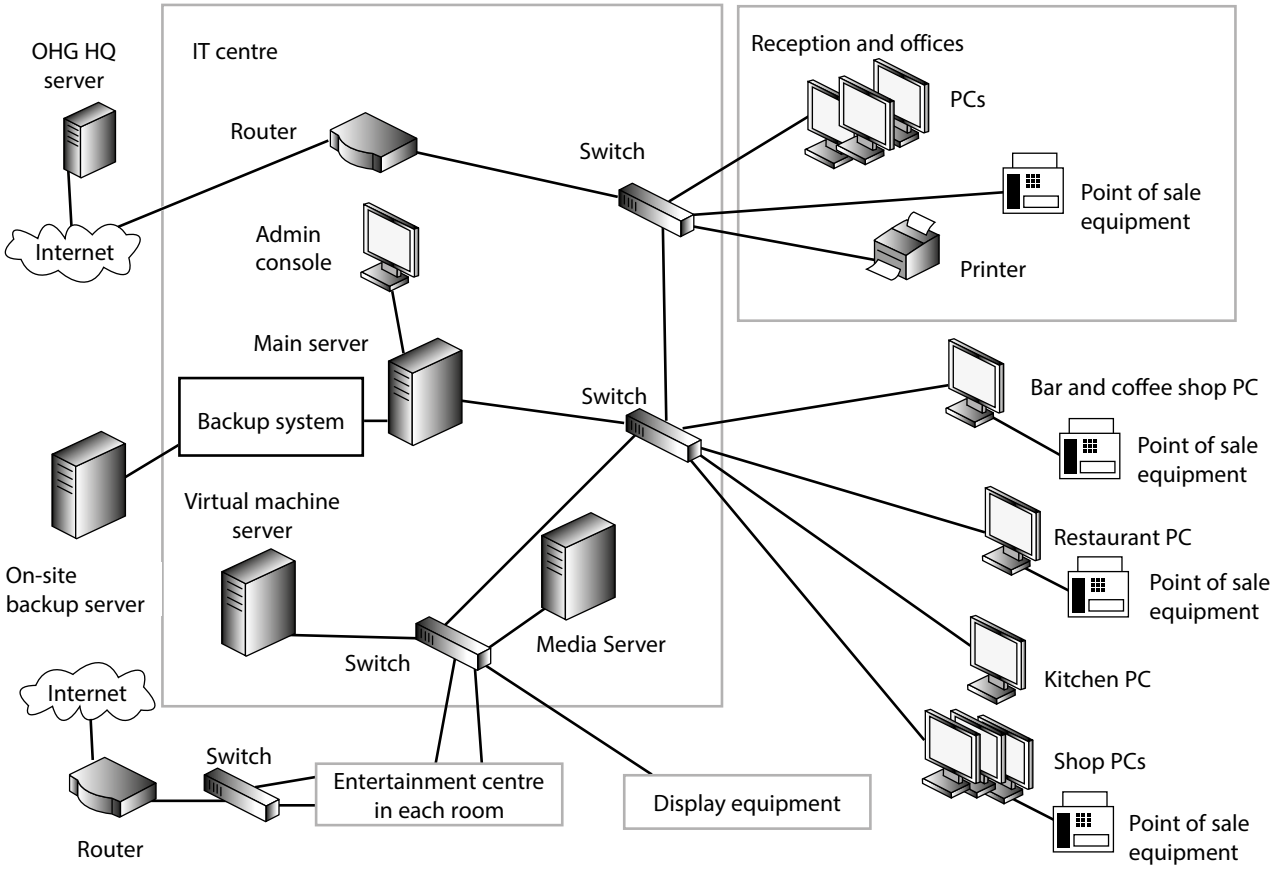

Figure 3

Peter has hired you to look at his plan and advise on cyber security and incident management.

Development plan

At a meeting with Peter you establish that:

1. No wireless communication will be available in the hotel except for short range systems required for contactless payments.
2. Internet access for guests will only be available by using their own devices. As there is no wireless available an Ethernet cable is supplied in each room.
3. The on-site backup server will be in the offices that are away from the reception area.
4. Internal cabling will use CAT6 cable.
5. Peter is concerned about the available bandwidth for internet and media streaming.
6. Point of sale equipment will be able to read contactless payment cards.
7. The display equipment will fetch content from the media server.
8. Some of the display equipment will allow user interaction via a trackball and/or keyboard.
9. Peter is concerned about having a robust backup system. He is thinking of using an on-site backup server and an internet connection to send more backups to a server at OHG's company HQ.
10. The network PCs and servers will run Linux.
11. The main server will act as the DHCP, mail, and file server.
12. The virtual machine and 386 emulation will be performed by open source software from a project that has been creating reliable emulation software for over 20 years.
13. The MS-DOS 3.2 software will run inside the 386 emulation.
14. The emulation software will mimic a good home PC from the mid 1980s, with a 16 MHz CPU, 4MB RAM and a 20MB hard drive.
15. Guests will have full access to MS-DOS, plus 1980s games and other applications.
16. Each entertainment centre will have a 3.5-inch, 720 KB floppy drive.
17. Guests who do not have a suitable floppy disc will be able to use an SD card in a 3.5-inch adaptor supplied by the hotel. Maximum file read/write sizes will be 720 KB.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

Peter has hired you to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template Risk_Assessment.rtf

Save your completed risk assessment as a PDF in your folder for submission as

activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS
TOTAL FOR PART A = 43 MARKS